REMARKS

Applicants have thoroughly considered the Examiner's remarks and the application has been amended to more clearly define the invention. Claims 1, 4-11, 13, 22 and 23 are presented in the application for further examination. Claims 1, 4, 6, 8, 9 and 13 have been amended by this Amendment A and claim 23 has been added. Reconsideration of the application claims as amended and in view of the following remarks is respectfully requested.

Before addressing the specific rejections, Applicants would like to point out some significant aspects of the invention. In general, the claimed invention provides a peer-to-peer (P2P) system and method over the Internet for simply and efficiently backing up files on one computer to another computer. Although storing files from one computer to another computer is known, as the Examiner has pointed out in the Second Copy 2000 reference, such storage has been across a known network and not on a peer-to-peer (P2P) basis over the Internet.

The prior art is not peer-to-peer within the context of the claimed invention. The invention does not employ a server to accomplish file transfer. The invention in one embodiment may employ a server to identify the Internet location of a second computer. However, it is the computing power and bandwidth of the first and second computers via the Internet rather than one or more servers which accomplish file transfer. The connection between first and second computers via the Internet for file transfer is P2P and direct. (For example, see definition of P2P: http://en.wikipedia.org/wiki/Peer_to_peer.)

There are several advantages of such a peer-to-peer system. For example, the claimed invention contemplates that the second computer is at a remote location from the first computer. As a result, back-up copies on the second computer are independent of the first computer. Since the first computer is intermittently connected to the second computer via the Internet, the second computer is not at risk if the first computer is at risk or if a network connected to the first computer fails or if a network interconnecting the first and second computers fails.

Going now to the Office action, the following remarks will follow the sequence of the Office action. The rejection directed to canceled claims 14-21 will not be addressed since these claims have been canceled. The rejection of claims 2 and 3 will be addressed with regard to claim 1 since claim 1 has been amended to include the subject matter of claims 2 and 3. The rejection of claim 12 will be addressed with regard to claim 9 since claim 9 has been amended to include the subject matter of claim 12.

Claims 1 and 9

Claims 1 and 9 stand rejected under 35 USC 102(b) as anticipated by Second Copy. Claim 1 has been amended to be directed to first and second computers connected via the Internet. In addition, claim 1 has been amended to recite that the first and second computers are Internet-enabled. In addition, claim 1 has been amended to recite that the identifying instructions identify the Internet address of the second computer. In addition, claim 1 has been amended to recite that the transferring instructions transfer back-up copies via the Internet directly.

Applicants acknowledge that the Second Copy 2000 reference indicates that backup copies can be stored "on storage devices on other computers across a network." However, Applicants respectfully submit that the invention recited by claim 1 is not anticipated by this vague statement. First, as noted above, claim 1 recites a P2P connection over the Internet whereas Second Copy only contemplates the transfer of files via a network. Although this reference generally contemplates network transfer, it does not contemplate Internet transfer which requires locating and using an IP address, as recited by amended claim 1.

To illustrate this aspect of the invention, paragraph 0026 and FIG. 1 have been amended to direct the specification and drawings to the Internet and claim 23 has been added to specify that the first and second computers are not connected by another network. Although the application initially contemplated both a communication network and/or the Internet to link the first and second computers, the application has been amended to be directed to the latter only. Applicants submit that Second Copy does not contemplate the amended claims.

Furthermore, the identifying instructions, the designating instructions and the transferring instructions as previously recited in canceled claims 2 and 3 have been included in amended claim 1. Among other things, this included language recites a destination identifier, designated storage schedule data and querying a server database for an IP address of the second computer.

Even if we assume that the Second Copy 2000 reference contemplates backup via the Internet, it is deficient because it is not enabling and fails to disclose such claim 1 features as follows:

(1) the identifying instructions to identify the Internet address of the second computer;

(2) the transferring instructions to transfer back-up copies via the Internet directly;

(3) a destination identifier;

(4) designated storage schedule data; and

(5) querying a server database for an IP address of the second computer.

Applicants submit that the Second Copy 2000 reference teaches away from invention. In particular, the reference states "Second Copy 2000's built-in auto-dial and auto-login features enable users to back up their files remotely to their servers …." Thus, Second Copy does not contemplate transfer of backup copies via the Internet directly from the first computer to the second computer.

Since the subject matter of claim 2 has been added to claim 1, the rejection of claim 2 will be addressed with respect to claim 1. Claim 2 has been rejected as follows:

As to dependent claim 2, "wherein the designating instructions include instructions for designating the one or more files to be transferred to the second computer; instructions for designating a destination identifier associated with the second computer; instructions for designating storage schedule data for back-up copies; and instructions for storing back-up copies of the designated one or more files, the designated destination identifier, and/or the designated storage schedule data in an originating database" is taught on page 1 of Second Copy, that the backups can be scheduled daily weekly, etc.

Applicants note that the language of claim 2, now in claim 1, does of claim not merely recite scheduling of backups as noted by the Second Copy 2000 reference. Instead, this language, now in amended claim 1, recites a destination identifier and a storage schedule data. These elements enable Internet operation and are not contemplated or suggested by the Second Copy 2000 reference. Applicants submit that this claim language distinguishes over the reference and request that the Examiner allow claim 1 at least for this reason.

Since the subject matter of claim 3 has been added to claim 1, the rejection of claim 3 will be addressed with respect to claim 1. Claim 3 has been rejected as follows:

As to dependent claim 3, "wherein the transferring instructions include retrieving storage schedule data to identify one or more back-up times for transferring back-up copies of the designated files from the first computer to the second computer" is shown in Second Copy on page 1 that backup can specify times;

"wherein the identifying instructions include retrieving the destination identifier for querying a server database to identify an Internet Protocol (IP) address of the second computer, said server database being located on a server linked to the first and second computer via the communication network, and wherein the transferring instructions use the identified IP address to initiate a communication session with the second computer via the communication network and to transfer the designated files at the designated back-up times" however '307 teaches that each vfiler is configured with IP addresses in col. 8, lines 41-59. The motivation to combine '307 and Second Copy is the same as stated above in claim 22.

Applicants note that the language of claim 3, now in claim 1, does not merely recite scheduling of backup times as vaguely suggested by the Second Copy 2000 reference. Instead, this language, now in amended claim 1, recites retrieving via the Internet. This element enables Internet operation and is not contemplated or suggested by the Second Copy 2000 reference. Applicants submit that this claim language distinguishes over the reference and request that the Examiner allow claim 1 at least for this reason.

Although the 307 reference relates to data recovery, it is deficient for the same reasons as noted above regarding the Second Copy 2000 reference. In particular, 307 contemplates a server in the form of a backup filer for storing backups and not P2P storage via the Internet, as recited by claim 1. Also, as noted below, the secondary considerations do not support combining the references as suggested by the Examiner.

In view of the above, Applicants request the allowance of amended claim 1.

Regarding claim 9, Applicants submit that it distinguishes over the Second Copy 2000 reference for at least the same reasons as claim 1 because both are directed to P2P transfers over the Internet. Further, since the subject matter of claim 12 has been added to claim 9, the

rejection of claim 12 will be addressed with respect to claim 9. Claim 12 has been rejected as follows:

> As to dependent claim 12, the following is not explicitly taught in the combination of teaching of Second Copy and '614: **"further comprising second transferring instructions executed by the second computer for transferring one or more stored files from the second computer back to the first computer in response to a retrieval request received from the first computer via the communication network"** however '307 teaches retrieving data in col. 5, lines 12-33.
>
> It would have been obvious to one of ordinary skill in the art at the time of the invention a scheduled backup system taught in Second Copy to include a means to identify the IP address of the remote computer. One of ordinary skill in the art would have been motivated to perform such a modification because a backup system is needed that can overcome the difficulties of prior backup methods see '307 (col. 1, lines 66 et seq.). "One way to copy a data set onto a backup filer to ensure against total primary filer failure is to physically move the storage disks from the primary filer to the backup filer. Another approach is to generate copies of the data set on backup tapes for use with the backup filer. However, these approaches can be slow and labor-intensive processes to manage. Yet another approach is to replicate a primary filer data set at the backup filer using a conventional storage replication technique, such as remote synchronous mirroring. In a remote synchronous replication environment, a mirrored data set must be transferred over a computer network and stored ("written") to the backup filer before the write operation completes on the primary filer. Although this technique assures a high level of data currency for the backup filer, it also introduces data latency issues as a result of, among other things, performance delays inherent to remote synchronous mirroring".

Amended claim 9 recites both the retrieval instructions and the second transferring instructions, in combination, which the Examiner admits is not explicitly taught by the Second Copy 2000 reference. The Examiner relies on the 307 reference to fill in the deficiency. However, as noted above, although the 307 reference relates to data recovery, it is deficient for the same reasons as noted above regarding the Second Copy 2000 reference. In particular, 307 contemplates a server in the form of a backup filer for storing backups and not P2P storage via

the Internet, as recited by the claim 9. Also, as noted below, the secondary considerations do not support combining the references as suggested by the Examiner.

In view of the above, Applicants request the allowance of amended claim 9.

Claims 4, 8 and 22

Claims 4, 8 and 22 stand rejected under 35 USC 103(a) over Second Copy in view of 307. Claim 22 has been amended to be directed to the combination of the computers and the server which facilitates transfer but is not in the file transfer loop. As pointed out above with regard to claims 1 and 9, both the Second Copy and 307 references are deficient in this regard so that claim 22 should be allowed.

Claim 4 recites instructions for displaying a form for designating files to be transferred. One feature of Applicant's invention is the user-friendly implementation as recited by claim 4. The Office action argues that the Second Copy reference are interpreted to be equivalent claim 4. However, there are no such instructions in Second Copy. In this regard, Second Copy is vague and not enabling so that Applicants request that this rejection be withdrawn.

Claim 4 recites a combination of elements not in the prior art. "[T]he question is whether there is something in the prior art as a whole to suggest the desirability, and thus the obviousness, of making the combination." Lindemann MaschinenFabrick GMBH v. American Hoist and Derrick Company, 730 F.2d 1452, 1462; 221 U.S.P.Q. 481, 488 (Fed. Cir.1984). As has been shown, the non-analogous teachings of the Second Copy 2000 reference are deficient. Therefore, nothing in the cited reference suggests the claimed combination including a form for user input. Indeed, the Examiner failed to cite any basis whatsoever for interpreting the Second Copy reference. In fact, the Examiner's rejection provides a text book example of impermissible hindsight analysis -- the Examiner used the invention as defined by the claims in order to reject the claims. See In re Oetiker, 977 F.2d at 1447; 24 U.S.P.Q.2d at 1446 ("There must be some reason, suggestion, or motivation found in the prior art whereby a person of ordinary skill in the field of the invention would make the combination. That knowledge can not come from the applicant's invention itself."). As indicated in the PTO Memorandum dated May 3, 2007 regarding the recent *KSR Int'l v. Teleflex, Inc.* Supreme Court decision:

(4) The Court noted that the analysis supporting a rejection under 35 U.S.C. § 103(a) should be made explicit, and that it was "important to identify a reason that would have prompted a person of ordinary skill in the relevant field to combine the [prior art] elements" in the manner claimed. The Court specifically stated:

> Often, it will be necessary . . . to look to interrelated teachings of multiple patents; the effects of demands known to the design community or present in the marketplace; and the background knowledge possessed by a person having ordinary skill in the art, all in order to determine whether there was an **apparent reason** to combine the known elements in the fashion claimed by the patent at issue. To facilitate review, this analysis **should be made explicit.**

KSR, slip op. at 14 (emphasis added).

Therefore, in formulating a rejection under 35 U.S.C. § 103(a) based upon a combination of prior art elements, it remains necessary to identify the reason why a person of ordinary skill in the art would have combined the prior art elements in the manner claimed.

Thus, the Office action must identify a reason other than the claims for the implicit interpretation of Second Copy and 307.

Claim 8 is directed to receiving instructions in combination with the instructions of claim 1. Claim 8 does not merely retrieve data, as suggested by the Office action, which points to a general teaching at 307, column 5, lines 12-33:

> Operationally, a request from a client **110** is forwarded as, e.g., a conventional CIFS or NFS protocol packet over the computer network **150** and onto a filer **300** where it is received at the network adapter **126**. A network driver of the media access layer **219** processes the packet, passes it onto the network protocol layers **212**-**216** and CIFS or NFS layer **218**, **220** for additional processing prior to forwarding to the WAFL layer **230**. Here, the WAFL file system generates operations to load (retrieve) the requested data from disk **130** if it is not resident "in core", i.e., in the memory **124**. If the information is not in memory, the WAFL layer **230** indexes into the inode file using the inode number to access an appropriate entry and retrieve a logical volume block number (VBN). The WAFL layer then passes the logical VBN to the disk storage (RAID) layer **224**, which maps that logical number to a disk block number and sends the latter to an appropriate driver (e.g., SCSI) of the disk driver layer **226**. The disk driver accesses the disk block number from disk **130** and loads the requested data block(s) in memory **124** for processing by the filer. Upon completion of the request, the filer (and operating system) returns a reply to the client **110** over the network **150**.

Unless a reference with such instructions in combination as recited by claim 8 can be cited, claim 8 must be allowed.

In view of the above, Applicants request the allowance of amended claims 4, 8 and 22.

Claims 5-7

Claims 5-7 stand rejected based on Second Copy in view of the 001 reference, column 1, lines 46-55 and column 9, lines 1-12. However, these portions of 001 teach away from the P2P invention as involving a separate storage system and not computer to computer P2P backups over the Internet. Thus, there is no basis for selectively combining 001 with Second Copy and the rejection must be withdrawn.

In view of the above, Applicants request the Examiner point to the specific claim elements in the prior art or allow claims 5-7.

Claims 10-11

Claims 10-11 stand rejected based on Second Copy in view of the 614 reference, column 11, lines 46-67; column 17, lines 14-16; and column 18, lines 53-59. Once again, Applicants respectfully submit that these claims recite structural elements in the context of P2P and the general teachings of 614 do not make obvious such recitals as "instructions for retrieving..." as required by claim 10 and "authentication instructions ..." as required by claim 11.

In view of the above, Applicants request the Examiner point to the specific claim elements in the prior art or allow claims 10-11.

Claim 13

Claim 13 stands rejected based on Second Copy in view of the 614 reference, column 17, lines 14-16; and column 18, lines 53-59. Once again, Applicants respectfully submit that this claim recites structural elements in the context of P2P and the general teachings of 614 do not make obvious the recitals of claim 13, such as "instructions for comparing..."

In view of the above, Applicants request the Examiner point to the specific claim elements in the prior art or allow claim 13.

SECONDARY CONSIDERATIONS

Finally, it is noted that secondary considerations point to the patentability of the claims
* and, specifically, to the conclusion that the claims are not obvious. Attached are pages 35-36 of *The Economist Technology Quarterly* published December 4, 2004 extolling the commercial success and technical success of P2P. For example, this article mentions at page 35, right column, last full paragraph, BitTorrent--a open source software project which distributes large files via P2P. This article is evidence of the secondary considerations of commercial success, long-felt need, and failure of others, pointing to the non-obviousness of the claims.

In view of the foregoing, favorable reconsideration and allowance of all claims is requested. The fact that Applicants may not have specifically traversed any particular assertion by the Office should not be construed as indicating Applicants' agreement therewith.

Applicants wish to expedite prosecution of this application. If the Examiner deems the application to not be in condition for allowance, the Examiner is invited and encouraged to telephone the undersigned to discuss making an Examiner's amendment to place the application in condition for allowance.

It is felt that a full and complete response has been made to the Office action and, as such, places the application in condition for allowance. Such allowance is hereby respectfully requested. If the Examiner feels, for any reason, that a personal interview will expedite the prosecution of this application, he is invited to telephone the undersigned.

The Commissioner is hereby authorized to charge any underpayment and credit any overpayment of government fees to Deposit Account No. 19-1345.

Respectfully submitted,

/Frank R. Agovino/

Frank R. Agovino, Reg. No. 27416
SENNIGER POWERS
One Metropolitan Square, 16th Floor
St. Louis, Missouri 63102
(314) 231-5400

FRA/caa
*Attachments

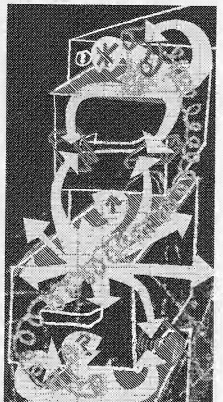
IMAGINE an ideal global information-storage system. It would have to be huge, capable of delivering any one of millions of files, some of them of enormous size, to anywhere in the world within moments. It would have to be self-configuring and self-healing, rather than centrally controlled, to ensure there was no single point of failure. And it would have to be secure, capable of supporting millions of users, while resisting constant assault both from physical attacks on its infrastructure and from malicious software circulated within the network.

Such a system sounds highly desirable, particularly when compared with the internet, which has become a piece of critical economic infrastructure but is beset by constant security scares and can become clogged up if too many users try to do the same thing at once. Yet this ideal system already exists, in the form of peer-to-peer (P2P) file-sharing networks such as eDonkey and KaZaA.

The technology, which is used by millions of music lovers to download songs—usually infringing copyrights—is reviled by the entertainment industry. In America and Europe, music and film companies are using the courts and lobbying for new laws to outlaw P2P technology. In October, trade groups representing the entertainment industry went so far as to petition America's Supreme Court to consider whether makers of P2P software should face "secondary liability" for copyright infringement by their users. Officials at America's Department of Justice have even suggested that using P2P supports terrorism. The technology is also condemned as a distribution system for illegal pornography.

Yet rather than being demonised, there are good reasons why the technology should be celebrated—and its benefits more widely studied and exploited. Arguing that the internet's robustness and security could be improved using technology generally associated with music piracy might seem strange, admits Yochai Benkler of Yale Law School, who raised the idea in a recent paper, but the suggestion is a tribute to "how robust these systems are". P2P networks have, after all, withstood years of legal, technical and physical assault, but still work.

The widespread equation of P2P with piracy has obscured the fact that the same technology is also being constructively applied in all sorts of fields, from content distribution and internet-routed phone calls to distributed storage and search.



In praise of P2P

Computing: Despite the legal wrangles over music piracy, peer-to-peer technology has many uses and is here to stay

Peer-to-peer technology is emerging as a powerful new approach to building large-scale computer systems, regardless of the entertainment industry's legal efforts.

Technically, "peer-to-peer" refers to a computer's ability to communicate directly with other computers running the same software, without having to go through intermediaries. While this might appear to describe the internet itself, the reality is slightly different. Although the internet was originally designed to be decentralised, it has evolved into more of a hub-and-spoke system. Personal computers at the edge of the network connect to powerful servers in the centre to do things such as send e-mails or retrieve web pages. What was once a network of equals, made up of machines that were both producers and consumers of content, became something that "looked like television with packets," says Clay Shirky, a technology consultant.

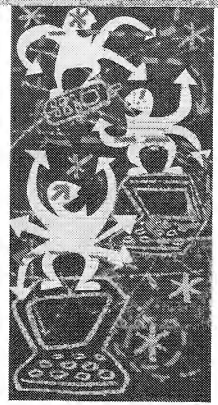
Strength in numbers

Peer-to-peer connects computers directly—and once enjoined, personal computers can do things they are unable to do alone. Most P2P systems let users pool resources, be it processing power, storage capacity or bandwidth. In the case of music file-sharing, users are, in effect, creating an enormous shared filing system from which they can all retrieve songs. Over half of all internet traffic is now generated by peer-to-peer applications, according to CacheLogic, a P2P network-services company in Britain. Figures from BigChampagne, an internet-research firm in Beverly Hills, California, suggest that at least 10% of the content on P2P networks is legal, and does not violate the entertainment industry's copyrights.

The most active P2P system, accounting for an estimated 35% of all internet traffic according to CacheLogic, is called BitTorrent. It is an open-source software project that is free to use and enables very large files to be stored and retrieved efficiently at essentially no cost. Though it is used for pirated music, it comes into its own when distributing really large files such as movies, games and large pieces of software such as the Linux operating system—things that would otherwise be very costly for companies or individuals to make available for download.

Part of BitTorrent's success stems from the way it creates incentives for users to give as well as to take. A study in 2000 on one P2P network showed that almost 70% of users never shared files, and around ››

"The equation of P2P with piracy has obscured its many virtuous uses."



half of the files available were offered by just 1% of users. BitTorrent is designed to remedy this. It rewards those who share files with others by increasing the download rate at which generous users can receive content, explains Bram Cohen, the system's creator. More sharing means there are more potential locations where copies of a given file are located, which in turn increases access speed. BitTorrent uses a technique called swarming, in which files are broken into small chunks that are then passed between peers. Two peers downloading the same file at the same time can also swap chunks they have already received from other peers, increasing the efficiency of the transfer.

P2P's ability to distribute content efficiently has prompted a number of initiatives to establish legal P2P distribution services. LionShare, devised at Penn State University, uses a file-sharing program to encourage the exchange of academic information around the world. Then there is Kontiki, a commercial P2P outfit, which was recently evaluated by the BBC as a way to distribute programmes online. Kontiki places portions of large files on participating PCs throughout the network, to increase performance. Computers at the edge of the network, not just big servers at the centre, thus help in the storage and sending of the file. Similarly, Red Swoosh runs a P2P network for legal file-sharing of copyrighted content. "Let's take this technology that the entertainment industry is scared of, and turn it into something that they want," says Travis Kalanick, Red Swoosh's chairman. Despite the legal rhetoric, the two sides are, in fact, quietly negotiating.

One organisation that relies on P2P content distribution is the Internet Archive, a public, non-profit library of digital content co-founded by Brewster Kahle, a technology entrepreneur based in San Francisco. The archive uses five different P2P systems so that it can distribute audio and video "without going broke on bandwidth fees", says Mr Kahle. Without P2P, he says, only big companies would be able to afford to distribute large amounts of video online. P2P allows individuals and non-profit initiatives like his to distribute multimedia content too.

Using a peer-to-peer approach for content distribution stands the traditional limitations of the internet on its head, says Cory Doctorow of the Electronic Frontier Foundation, a high-tech lobby group. P2P does away with the "popularity penalty" that makes desirable content difficult to obtain. With systems such as BitTorrent, the more a file is in demand, the more available it becomes. Content automatically ends up being stored close to the users who request it, improving the performance of the system.

But there is more to P2P than just distributing information efficiently. The same approach has inspired other applications. The creators of KaZaA, a popular P2P network mainly used to share music and video files, sold the company and set up Skype, a free internet-telephony service that uses a similar P2P architecture to route voice calls rather than music files from one PC to another. (Both KaZaA and Skype rely on the idea that some computers should appoint themselves as "supernodes", akin to voluntary traffic police, to ensure a smooth flow of data between other machines on the network.)

Another company, Groove Networks, uses a P2P-like system to provide shared workspaces for online collaboration: it allows, for example, more than one person to edit the same document simultaneously. P2P is also an obvious way to construct an internet-based file back-up service. And why not build a search engine based on P2P principles that recommends documents based on other users' preferences, much as Amazon recommends books based on other customers' purchases? "P2P is a perfectly natural evolution of the internet—in fact, a return to the original style and usage that the creators of the internet really had in mind," explains Ian Clarke, the founder of FreeNet, a P2P network that provides anonymity in order to bypass censorship.

Appropriately enough given the internet's military origins, the American army is also looking into the uses of P2P technology on the battlefield, to improve the "situational awareness" of its troops. Rather than distributing information in a hierarchical manner, it might make more sense for soldiers to exchange data using a P2P approach. (Some military radios already work in this way: they use a self-configuring technique called "mesh networking", where each radio also acts as a relay to interconnect other nearby radios.)

With all this resource sharing and decentralisation going on, one might be tempted to think the internet is finally becoming one big happy community, as some of its more optimistic visionaries had hoped. Alas, bursting that bubble is Bernardo Huberman, the director of the Information Dynamics Lab at Hewlett-Packard Laboratories. "P2P is an architecture—what we need is a market mechanism," he says. That way, P2P users can be properly compensated for sharing their computing cycles, storage capacity or bandwidth with others. His researchers have, for example, devised a system called Tycoon, which auctions off spare computing capacity. This sort of approach, he argues, is vital if P2P applications are to develop from today's volunteer systems into something big firms might want to adopt. "If you noticed coins dropping into your machine, you might be tempted to do that," he says.

Peer pressure

The danger is that the legal efforts to stamp out P2P's illegal uses might also blight the prospects for its virtuous uses, by hindering investment. In the case of Napster, once the most popular P2P music-sharing service, a legal ruling in 2001 temporarily shut the company down, and its venture-capital backers were sued for vicarious liability. This dampened investors' willingness to fund other firms developing P2P-related technology, even though there are now plenty of examples of legal uses of P2P.

Meanwhile, the technologists are continuing to write their software code. "P2P doesn't need a case made in its favour—it's just technology. Once it's out of the box you can't put it back in the box, and that's the end of that," says Mr Cohen—speaking, as you would expect of a P2P pioneer, over Skype's P2P telephone network. ■